



FortiClient EMS - QuickStart Guide

Version 6.0.3

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<https://cookbook.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



November 23, 2018

FortiClient EMS 6.0.3 QuickStart Guide

04-603-478342-20181123

TABLE OF CONTENTS

Introduction	5
Supported installation platforms	5
Requirements	5
Required services and ports	6
Deployment options	7
Standalone	8
Integrated with FortiGate	8
Chromebook setup	9
G Suite account	9
SSL certificates	9
How FortiClient EMS and FortiClient work with Chromebooks	9
Installation	11
Downloading the installation file	11
Installing FortiClient EMS	11
Extending license expiries	13
Starting FortiClient EMS and logging in	13
Accessing FortiClient EMS remotely	13
Windows, macOS, and Linux Endpoint Management Setup	15
FortiClient EMS	15
FortiClient EMS integrated with FortiGate	16
Configuring user accounts	17
Adding endpoints	17
Creating gateway lists	19
Assigning gateway lists to endpoints	20
Creating FortiClient installers	20
Configuring endpoint profiles	23
Preparing Windows endpoints for FortiClient deployment	27
Assigning profiles to Windows, macOS, and Linux endpoints	28
Viewing endpoints	28
Viewing the Endpoints content pane	28
Using the quick status bar	32
Viewing endpoint details	33
FortiClient EMS for Chromebooks Setup	34
Google Admin Console setup	34
Logging into the Google Admin console	34
Adding the FortiClient Web Filter extension	35
Configuring the FortiClient Web Filter extension	35
Adding root certificates	36
Disabling access to Chrome developer tools	38
Disallowing incognito mode	39
Disallowing guest mode	39
Blocking Task Manager	40
Service account credentials	41

Configuring default service account credentials	41
Configuring unique service account credentials	42
Adding SSL certificates	47
Adding SSL certificates to FortiClient EMS for Chromebook endpoints	47
Adding Google domains	48
Configuring Chromebook profiles	48
Adding new profiles	48
Enabling/disabling safe search	49
Assigning profiles to Chromebooks	50
Viewing domains	50
Viewing the Google Users pane	50
Viewing user details	51
Change Log	53

Introduction

This guide describes how to install and set up FortiClient Enterprise Management Server (EMS) for the first time. FortiClient EMS is used to deploy and manage FortiClient endpoints. This guide also describes how to set up the Google Admin console to use the FortiClient Web Filter extension. Together the products also provide web filtering for Google Chromebook users.



An informative video introducing you to FortiClient EMS is available in the [Fortinet Video Library](#).

Supported installation platforms

You can install FortiClient EMS on the following platforms:

- Microsoft Windows Server 2008 R2 or newer



For information about minimum system requirements and supported platforms, see the *FortiClient EMS Release Notes*, available in the [Fortinet Document Library](#).

Requirements

The following components and knowledge are required to use FortiClient EMS for managing Chromebooks:

- FortiClient EMS installer
- FortiClient Web Filter extension available in the Google Web Store for Chrome OS
- G Suite account
- Knowledge of administering the Google Admin console
- A domain configured in the Google Admin console
- SSL certificate to support communication between FortiClient Web Filter extension and FortiClient EMS
- SSL certificate to support communication between FortiClient Web Filter extension and FortiAnalyzer for logging, if using
- Unique set of service account credentials

Required services and ports

You must ensure required ports and services are enabled for use by FortiClient EMS and its associated applications on your server. The required ports and services enable FortiClient EMS to communicate with endpoints and servers running associated applications. You do not need to enable ports 8013 and 10443 as the FortiClient EMS installation opens these.

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient Telemetry	FortiClient endpoint management	TCP	8013 (default)	Incoming	Installer/GUI
Samba (SMB) service	FortiClient EMS uses the SMB service during FortiClient initial deployment.	TCP	445	Outgoing	N/A
Distributed Computing Environment / Remote Procedure Calls (DCE- RPC)	The EMS server connects to endpoints using RPC for FortiClient initial deployment.	TCP	135	Outgoing	N/A
Active Directory server connection	Retrieving workstation and user information	TCP	389 (LDAP) or 636 (LDAPS)	Outgoing	GUI
FortiClient download	Downloading FortiClient installer created by the EMS server	TCP	10443 (default)	Incoming	Installer
Apache/HTTPS	Web access to EMS	TCP	443	Incoming	Installer
FortiGuard	FortiGuard antivirus, vulnerability, and application version updates	TCP	80	Outgoing	N/A
SMTP server/email	Alerts for EMS and endpoint events. When an alert is triggered, an email notification is sent	TCP	25 (default)	Outgoing	GUI
FortiClient endpoint probing	FortiClient EMS uses ICMP for endpoint probing during FortiClient initial deployment.	ICMP	N/A	Outgoing	N/A

The following ports and services are only applicable when using FortiClient EMS to manage Chromebooks:

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient on Chrome OS	Connection to EMS	TCP	8443 (default) You can customize this port.	Incoming	GUI
G suite API/Google domain directory	API calls to retrieve Google domain information	TCP	443	Outgoing	N/A

The following ports and services should be enabled for use on Chromebooks when using FortiClient for Chromebooks:

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient EMS	Connection to profile server	TCP	8443 (default)	Outgoing	Via Google Admin console when adding the profile
FortiGuard	URL rating	TCP	443, 3400	Outgoing	N/A
FortiAnalyzer	Send logs to FortiAnalyzer	TCP	8443	Outgoing	N/A

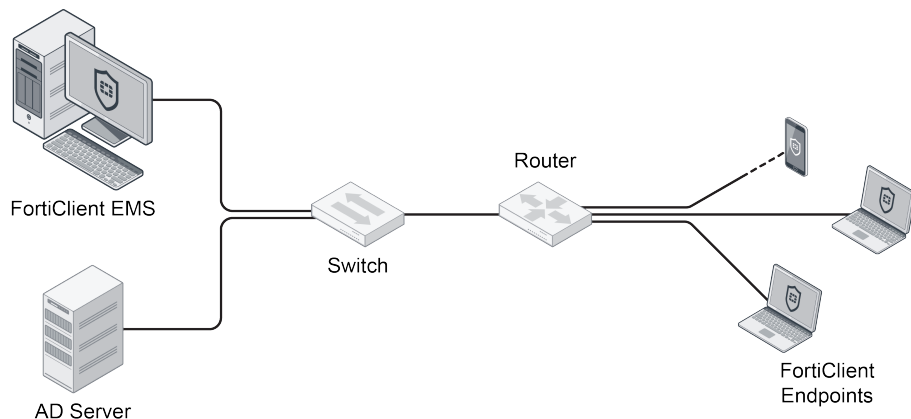


For the list of required services and ports for FortiClient, see the *FortiClient Administration Guide* on the [Fortinet Document Library](#).

Deployment options

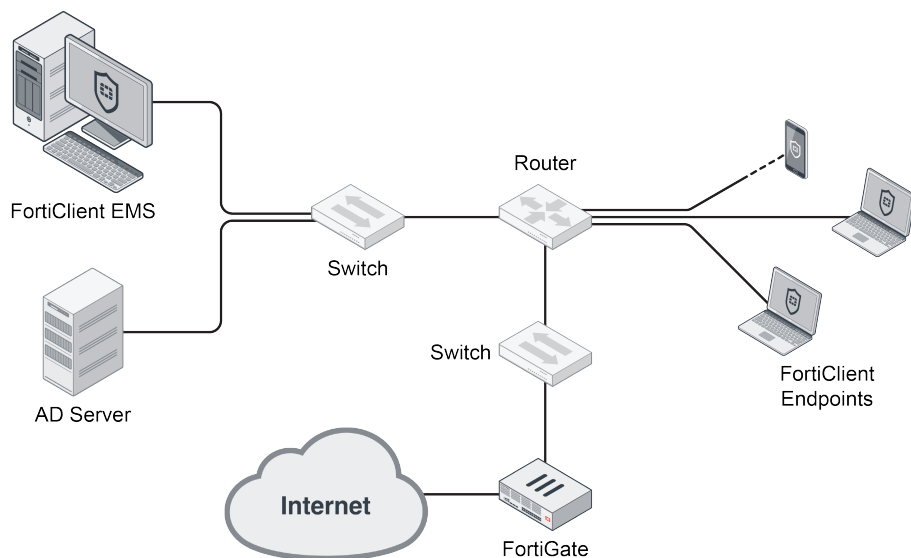
The following deployment options for EMS are supported: standalone or integrated with FortiGate.

Standalone



In standalone mode, a FortiGate device is not required, and network access control (NAC) is not supported. In standalone mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to EMS to receive configuration information from EMS. EMS is used to deploy, configure, and monitor FortiClient endpoints.

Integrated with FortiGate



In integrated mode, a FortiGate device is required, and NAC is supported. In integrated mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to FortiGate to receive compliance rules. FortiClient endpoints also connect to EMS to be managed. After FortiClient endpoints are connected, compliance rules are downloaded from FortiGate to the endpoint. EMS might also push a profile of FortiClient configuration information to endpoints. FortiClient endpoints are now managed, and NAC is enforced.

FortiClient uses the compliance rules from FortiGate to communicate whether the endpoint is compliant. If an endpoint fails to meet the compliance rules, the steps required to remain compliant are communicated. For more information, see the *FortiClient Administration Guide*.

Chromebook setup

The following sections are only applicable if you plan to use FortiClient EMS to manage Chromebooks:

G Suite account

You need to sign up for your G Suite account before you can use the Google service and manage your Chromebook users.

The G Suite account is different from the free consumer account. The G Suite account is a paid account that gives access to a range of Google tools, services, and technology.

You can sign up for a G Suite account [here](#).

In the sign up process, you must use your email address to verify your Google domain. This also proves you have ownership of the domain.

SSL certificates

FortiClient EMS requires an SSL certificate signed by a Certificate Authority (CA) in pfx format. Use your CA to generate a certificate file in pfx format, and remember the configured password. For example, the certificate file name is *server.pfx* with password 111111.

The server where FortiClient EMS is installed should have a fully qualified domain name (FQDN), such as *ems.forticlient.com*, and you must specify the FQDN in your SSL certificate.

If you are using a public SSL certificate, the FQDN can be included in *Common Name* or *Subject Alternative Name*. You must add the SSL certificate to FortiClient EMS. See [Adding SSL certificates to FortiClient EMS for Chromebook endpoints on page 47](#). You do not need to add the root certificate to the Google Admin console.

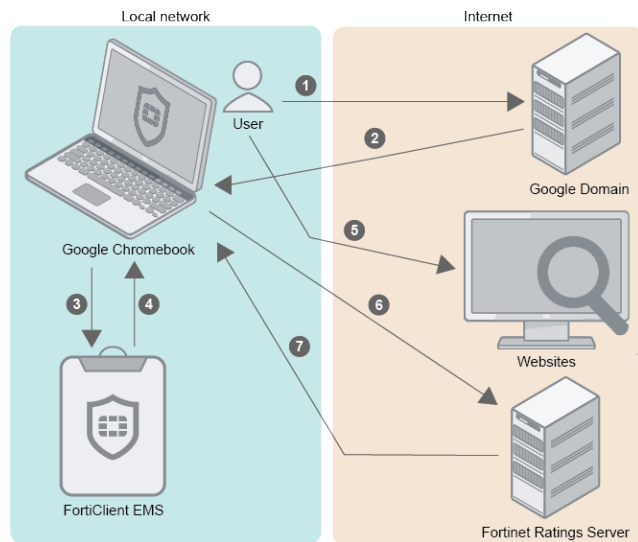
If you are using a self-signed certificate (non-public SSL certificate), your certificate's *Subject Alternative Name* must include *DNS:<FQDN>*, for example, *DNS:ems.forticlient.com*. You must add the SSL certificate to FortiClient EMS and the root certificate to the Google Admin console to allow the extension to trust FortiClient EMS. See [Adding root certificates on page 36](#).

How FortiClient EMS and FortiClient work with Chromebooks

After you install and configure FortiClient EMS, the Google Admin console, and the FortiClient Web Filter extension, the products work together to provide web filtering security for Google Chromebook users logged into the Google domain. Following is a summary of how the products work together after setup is complete:

1. A user logs into the Google Chromebook.
2. The Google Chromebook downloads the FortiClient Web Filter extension.
3. FortiClient connects to FortiClient EMS.
4. FortiClient downloads a profile to the Google Chromebook. The profile contains web filtering settings from FortiClient EMS.
5. The user browses the Internet on the Google Chromebook.
6. FortiClient sends the URL query to the Fortinet Ratings Server.

7. The Fortinet Ratings Server returns the category result to FortiClient. FortiClient compares the category result with the profile to determine whether to allow the Google Chromebook user to access the URL.



Installation

For a complete endpoint solution, FortiClient should be installed on all endpoints, and FortiClient EMS should be installed for central management and provisioning of endpoints.

Following is a summary of how to install and start FortiClient EMS:

1. Download the installation file. See [Downloading the installation file on page 11](#).
2. Install FortiClient EMS. See [Installing FortiClient EMS on page 11](#).
3. Start FortiClient EMS and log in. See [Starting FortiClient EMS and logging in on page 13](#).

For information about upgrading FortiClient EMS, see the FortiClient EMS *Release Notes*.



An instructional video on how to install, log in, and change your administrator password is available in the [Fortinet Video Library](#).

Downloading the installation file

FortiClient EMS is available for download from the [Fortinet Support website](#).

You can also receive the installation file from a sales representative.

The following installation file is available for FortiClient EMS:

FortiClientEnterpriseManagement_6.0.3.<build>_x64.exe

For information about obtaining FortiClient EMS, contact your Fortinet reseller.

Installing FortiClient EMS

The FortiClient EMS installation package includes:

- FortiClient EMS
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server



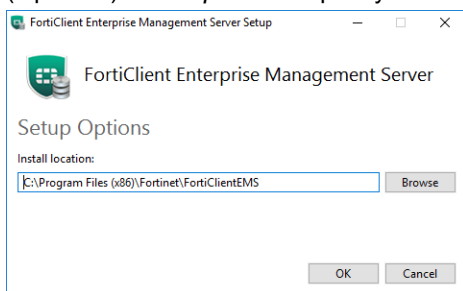
Local administrator rights and Internet access are required to install FortiClient EMS.

1. If you are logged into the system as an administrator, double-click the downloaded installation file.
If you are not logged in as an administrator, right-click the installation file, and select *Run as administrator*.

2. If applicable, select **Yes** in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select **I agree to the license terms and conditions** if you agree with the license terms and conditions. If you do not agree, you cannot install the software.

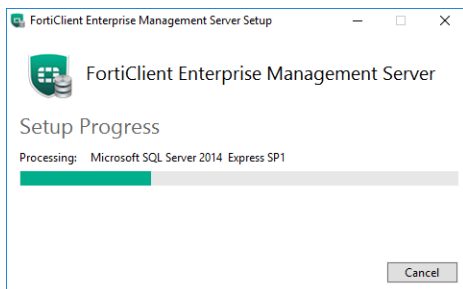


4. (Optional) Click **Options** to specify a custom directory for the FortiClient EMS installation.

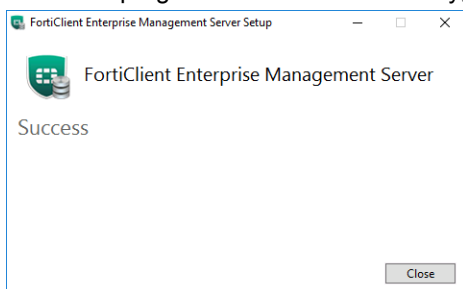


- a. Click **Browse** to locate and select the custom directory.
 - b. Click **OK** to return to the installation wizard.
5. Click **Install**.

The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others.



6. When the program has installed correctly, the *Success* window displays. Click **Close**.



A *FortiClient Enterprise Management Server* icon is added to the desktop.

Extending license expiries

You can apply multiple licenses to your FortiClient EMS to extend the license expiry. For example, consider you purchase two one-year licenses for FortiClient EMS. After you register and apply the first license, FortiClient EMS has an expiry date of August 1, 2018. You can register and apply the second license as a renewal, after which FortiClient EMS has an expiry date of August 1, 2019.

Note you must upload the second license file to FortiClient EMS using the GUI. Registering the license does not automatically update the license expiry in FortiClient EMS.



Using a second license to extend the license expiry date does not increase the number of licensed clients. To increase the number of licensed clients, contact [Fortinet Support](#) for a co-term contract.

For details, see the *FortiClient EMS Administration Guide*.

Starting FortiClient EMS and logging in

FortiClient EMS runs as a service on Windows computers.

1. Double-click the *FortiClient Enterprise Management Server* icon.
2. Sign in with the username *admin* and no password.
3. Change the username and password by going to *Administration > Administrators*.
4. Configure FortiClient EMS by going to *System Settings*.

Accessing FortiClient EMS remotely

You can access FortiClient EMS remotely using a web browser instead of the GUI.

To enable remote access to FortiClient EMS:

1. Go to *System Settings > Server*.
2. Enable *Remote HTTPS access*.
3. If desired, in the *Custom hostname* box, enter the host name or IP address. Otherwise, the *Pre-defined hostname* is used.
4. If desired, select the *Redirect HTTP request to HTTPS* checkbox. If this option is enabled, if you attempt to remotely access EMS at *http://<server_name>*, this is automatically redirected to *https://<server_name>*.
5. Click *Save*.

To remotely access FortiClient EMS:

- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`
Ensure you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Windows, macOS, and Linux Endpoint Management Setup

This section describes how to set up FortiClient EMS for Windows, macOS, and Linux endpoint management. It provides an overview of using FortiClient EMS and FortiClient EMS integrated with FortiGate.

When FortiClient EMS is integrated with FortiGate, you can use gateway lists to help FortiClient endpoints connect to FortiClient EMS and FortiGate. You can also import FortiClient profiles from FortiGate to FortiClient EMS.

FortiClient EMS

Following is a summary of how to use FortiClient EMS without FortiGate:

1. Configure user accounts. See [Configuring user accounts on page 17](#).
2. Add domains and/or discover local endpoints. See [Adding endpoints on page 17](#)
3. Add a FortiClient installer to EMS. See [Creating FortiClient installers on page 20](#).
4. Create an endpoint profile and select a FortiClient installer. See [Creating profiles to deploy FortiClient on page 24](#).



FortiClient EMS can deploy FortiClient (Windows) to Active Directory endpoints that do not have FortiClient installed, as well as upgrade existing FortiClient installations if the endpoints are already connected to the EMS server. To allow initial deployment, EMS must be able to resolve the endpoint IP address via the DNS configured on the server.



You can use with workgroups only to upgrade FortiClient (Windows) on endpoints after they connect Telemetry to EMS and FortiClient connects to . When using workgroups, you must separately install FortiClient (Windows) on endpoints. See the *Administration Guide*.



You can use FortiClient EMS to replace, upgrade, and uninstall FortiClient (macOS) after they connect Telemetry to EMS and FortiClient connects to FortiClient EMS. You cannot use FortiClient EMS to initially deploy FortiClient (macOS) and must separately install it on endpoints. See the *FortiClient EMS Administration Guide*.

-
5. Prepare Windows endpoints for FortiClient deployment. See [Preparing Windows endpoints for FortiClient deployment on page 27](#).

You must also prepare the Windows AD server for deployment. See the *FortiClient EMS Administration Guide*.

6. Assign a profile to a workgroup, domain, endpoint group, or organizational group. See [Assigning profiles to Windows, macOS, and Linux endpoints on page 28](#).

Depending on the selected profile's configuration, FortiClient is installed on the endpoints to which the profile is applied.

After FortiClient installation, the endpoint user must connect FortiClient Telemetry to FortiGate or FortiClient EMS to receive the profile configuration and complete endpoint management setup. See [Connecting manually from FortiClient on page 19](#).

7. View the endpoint status. See [Viewing endpoints on page 28](#).

FortiClient EMS integrated with FortiGate

Following is a summary of how to use FortiClient EMS when integrated with FortiGate:

1. Configure user accounts. See [Configuring user accounts on page 17](#).
2. Add domains and/or discover local endpoints. See [Adding endpoints on page 17](#).
3. Create gateway lists. See [Creating gateway lists on page 19](#).
4. Assign the lists to domains or workgroups. See [Assigning gateway lists to endpoints on page 20](#).
Alternately, you can add a FortiClient Telemetry gateway list to a custom FortiClient installer using the FortiClient Configurator tool.
5. Add a FortiClient installer to EMS. See [Creating FortiClient installers on page 20](#).
6. Create an endpoint profile and select a FortiClient installer. See [Creating profiles to deploy FortiClient on page 24](#).



FortiClient EMS can deploy FortiClient (Windows) to Active Directory endpoints that do not have FortiClient installed, as well as upgrade existing FortiClient installations if the endpoints are already connected to the EMS server. To allow initial deployment, EMS must be able to resolve the endpoint IP address via the DNS configured on the server.



You can use with workgroups only to upgrade FortiClient (Windows) on endpoints after they connect Telemetry to EMS and FortiClient connects to . When using workgroups, you must separately install FortiClient (Windows) on endpoints. See the *Administration Guide*.



You can use FortiClient EMS to replace, upgrade, and uninstall FortiClient (macOS) after they connect Telemetry to EMS and FortiClient connects to FortiClient EMS. You cannot use FortiClient EMS to initially deploy FortiClient (macOS) and must separately install it on endpoints. See the *FortiClient EMS Administration Guide*.

-
7. Prepare Windows endpoints for FortiClient deployment. See [Preparing Windows endpoints for FortiClient deployment on page 27](#).
You must also prepare the Windows AD server for deployment. See the *FortiClient EMS Administration Guide*.
 8. Assign a profile to a workgroup, domain, endpoint group, or organizational group. See [Assigning profiles to Windows, macOS, and Linux endpoints on page 28](#).
Depending on the selected profile's configuration, FortiClient is installed on the endpoints to which the profile is applied.
After FortiClient installation, the endpoint user must connect FortiClient Telemetry to FortiGate or FortiClient EMS to receive the profile configuration and complete endpoint management setup. See [Connecting manually from FortiClient on page 19](#).
 9. View the endpoint status. See [Viewing endpoints on page 28](#).

Configuring user accounts

You can configure users to have no access or administrator access to FortiClient EMS. You can configure local Windows users, LDAP users, or local Windows users and LDAP users.

For local Windows users, the user list is derived from the server where FortiClient EMS is installed. If you want to add more users, you must add them to the server.

For LDAP users, you must add an LDAP server to FortiClient EMS, then configure users.

To add an LDAP server:

1. Go *Administration > User Server*.
2. Configure the options, and click *Test*.
3. If the test is successful, click *Save*.

To configure users:

1. Go to *Administration > Administrators*.
2. Click *Add* from the toolbar.
3. In the *User* list, select *Windows* or *LDAP*.
The *LDAP* option is available only after you add an LDAP server to FortiClient EMS.
4. Select the user's specific domain access.
5. Configure the permissions.
6. Click *Save*.

Adding endpoints

You can add endpoints using an Active Directory service. Endpoints are also added when endpoint users manually connect FortiClient Telemetry to FortiClient EMS.

Adding endpoints using an Active Directory domain server

Endpoints can be manually imported from an AD server. You can import and synchronize information about computer accounts with an LDAP or LDAPS service. You can add endpoints by identifying endpoints that are part of an AD domain server.



An instructional video on how to add a domain is available in the [Fortinet Video Library](#).



You can add the entire domain or an organizational unit (OU) from the domain.

1. Go to *Endpoints > Manage Domains > Add*. The *Domain* pane displays.

2. Configure the following options:

IP address/Hostname	Enter the domain's IP address or hostname.
Port	Enter the port number.
Distinguished name	Enter the distinguished name (optional).
Bind type	Select the bind type: <i>Simple</i> , <i>Anonymous</i> , or <i>Regular</i> . When you select <i>Regular</i> , you must enter the <i>Username</i> and <i>Password</i> .
Username	Available when <i>Bind Type</i> is set to <i>Regular</i> . Enter the username.
Password	Available when <i>Bind Type</i> is set to <i>Regular</i> . Enter the user password.
Show Password	Available when <i>Bind Type</i> is set to <i>Regular</i> . Turn on and off to show or hide the password.
LDAPS connection	Turn on to enable a secure connection protocol when <i>Bind Type</i> is set to <i>Regular</i> .
Sync every	Enter the sync schedule between FortiClient EMS and the domain in minutes. The default is ten minutes.

3. Click *Test* to test the domain settings connection.
4. If the test is successful, select *Save* to save the new domain. If not, correct the information as required, then test the settings again.



After importing endpoints from an AD server, you can edit the endpoints. These changes are not synced back to the AD server.

Connecting manually from FortiClient

Endpoint users can manually connect FortiClient Telemetry to FortiClient EMS by specifying the IP address for FortiClient EMS in FortiClient. This process is sometimes called registering FortiClient to FortiClient EMS.

1. In FortiClient Console on the endpoint, go to the *Compliance & Telemetry* tab.
2. In the *FortiGate or EMS IP* box, enter the EMS IP address, and click *Connect*.
FortiClient connects to FortiClient EMS.

For information about FortiClient, see the [FortiClient Administration Guide](#).



The FortiClient Telemetry gateway port may be appended to the gateway list address on FortiClient and separated by a colon. When the port is not provided, FortiClient attempts to connect to the IP address given using the default port. The default connection port in FortiClient 5.2 is 8010 and in FortiClient 5.4 and 6.0 is 8013. By default, FortiClient EMS listens for connection on port 8013.



It is considered best practice to add endpoints using the method in [Adding endpoints using an Active Directory domain server on page 17](#). Connecting FortiClient to FortiClient EMS manually is only recommended for troubleshooting purposes.

Creating gateway lists

You can create a gateway list that contains IP addresses for multiple FortiGate units. FortiClient searches for IP addresses in its subnet in the gateway IP list and connects to the FortiGate in the list that is in the same subnet as the host system.

If FortiClient cannot find any FortiGates in its subnet, it attempts to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as it was configured in the gateway list.

1. Go to *Gateway Lists > Manage Gateway Lists*.
2. Click the *Add* button.

The screenshot shows the FortiClient Enterprise Management Server interface. On the left is a navigation menu with options: Dashboard, Endpoints, Quarantine Management, Software Inventory, Endpoint Profiles, Profile Components, Gateway Lists (selected), Manage Gateway Lists, head-office, Administration, and System Settings. The main content area is titled 'Gateway List' and contains the following fields:

- Name:** Required (text input field)
- Comment:** Optional (text input field)
- IP addresses/Hostnames:** Press enter to add a new value... (text input field)
- Connect to local subnets only:** ☐
- Use connection key:** ☐
- Managed by EMS:** 10.0.4.103:8013 (dropdown menu)

Below the dropdown menu, there is a note: 'All registered FortiClients can be managed by this EMS server. Configurable via System Settings > Server > Listen on IP'. At the bottom right of the form is a green 'Save' button.

3. Configure the following:

Name	Enter the list name.
Comment	Enter additional comments (optional).
IP addresses/Hostnames	Enter the IP address(es) or hostname(s) of the FortiGate devices. You can also use an FQDN. Press the <i>Enter</i> key to add additional IP addresses.
Connect to local subnets only	Enable to only allow connection to local subnets.
Use connection key	Enable the connection key endpoints can use to connect to FortiGate units.
New connection key	Enter the connection key.
Confirm new connection key	Reenter the connection key to confirm.
Managed by EMS	Select an option from the dropdown list. Users can configure this IP address in <i>System Settings > Server</i> .

4. Click **Save**.

Assigning gateway lists to endpoints

After creating a gateway list, you can assign the list to endpoints. When you assign the IP list and FortiClient Telemetry data connection process has started, the endpoint connects to a FortiGate or EMS, based on the gateway list.

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Assign gateway list*.
3. Select the desired list or create a new gateway list.

Creating FortiClient installers

When you create a FortiClient installer to FortiClient EMS, you can specify what FortiClient features to include in the installer for the endpoint. You can include a feature in the installer, then disable the feature in the profile. Because the feature is included in the installer, you can update the profile later to enable the feature on the endpoint.

For example, consider that you create an installer that has SSL VPN and IPsec VPN enabled. You then assign the installer to a profile where VPN is disabled. The endpoints that the profile is deployed to will have VPN disabled. At a later time, if you enable VPN on the profile, the endpoints will then have VPN enabled, since it was included in the installer.

When you create a FortiClient installer in FortiClient EMS, an installer for the Windows operating system and an installer for the macOS operating system are added to FortiClient EMS.



After you add a FortiClient installer to FortiClient EMS, you cannot edit it. You can delete the installer from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.

1. Go to *Profile Components > Manage Installers*.
2. Click *Add*.
3. On the *General* tab, set the following options.

Add Installer

General Features Advanced Telemetry

Name
Required

Notes

Version
6.0

Patch version
6.0.2

☐ Keep updated to the latest patch

Quit Back Next Save

Name	Enter the FortiClient installer's name.
Notes	(Optional) Enter any notes about the FortiClient installer.
Version	Select the FortiClient version to install. Click <i>Upload</i> to add a custom FortiClient installer.
Patch version	Select the specific FortiClient patch version to install.
Keep updated to the latest patch	Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint. This field is only available for the latest FortiClient version FortiClient EMS can access from FortiGuard. This option is not available if an older FortiClient version is selected.

4. Click *Next*. On the *Features* tab, set the following options.

Add Installer

General Features Advanced Telemetry

Basic Security Features

- ☒ Security Fabric Agent (Mandatory Feature)
Endpoint telemetry, host vulnerability scanning, and remediation.
- ☒ Secure Access Architecture Components
SSL and IPsec VPN
- ☐ Advanced Persistent Threat (APT) Components
FortiSandbox detection and quarantine features (Windows only)

Additional Security Features

- ☐ AntiVirus
- ☐ Web Filtering
- ☐ Application Firewall
- ☐ Single Sign-On mobility agent

Quit Back Next Save

Security Fabric Agent (Mandatory Feature)

Enabled by default and cannot be disabled. Installs FortiClient with Telemetry and Vulnerability Scanning enabled.

Secure Access Architecture Components

Enable to install FortiClient with SSL VPN and IPsec VPN enabled. Disable to omit SSL VPN and IPsec VPN support from the FortiClient installer.

Advanced Persistent Threat (APT) Components

Enable to install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient installer. Includes FortiSandbox detection and quarantine features.

Additional Security Features

Enable to select one, two, or all of the following features:

- AntiVirus
- Web Filtering
- Application Firewall
- Single Sign-On mobility agent

Disable to exclude the features from the FortiClient installer.

5. Click *Next*. On the *Advanced* tab, set the following options.

Add Installer

General Features Advanced Telemetry

Advanced options

- ☐ Enable automatic registration
- ☐ Enable desktop shortcut
- ☐ Enable start menu shortcut
- ☐ Enable endpoint tag

Quit Back Next Save

Enable automatic registration	Enable to configure FortiClient to automatically connect Telemetry to EMS or FortiGate after FortiClient is installed on the endpoint. Disable to turn off this feature and require endpoint users to manually connect Telemetry to EMS or FortiGate.
Enable desktop shortcut	Enable to configure the FortiClient installer to create a desktop shortcut on the endpoint.
Enable start menu shortcut	Enable to configure the FortiClient installer to create a Start menu shortcut on the endpoint.
Enable endpoint tag	<p>Enable to configure an endpoint tag to assign to endpoints. Under <i>Endpoint Tag</i>, select an existing tag or enter a new tag. FortiClient EMS automatically groups tagged endpoints according to group assignment rules. For more information, see the FortiClient EMS Administration Guide.</p> <p>This option is not available when the FortiClient installer selected or uploaded in step 3 is a version prior to 6.0.0.</p>

6. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the EMS server, which will manage FortiClient once it is installed on the endpoint. Also set the following option.

Connect Telemetry to Security Fabric (FortiGate)	<p>Enable this option, and select the name of the gateway list to use. The gateway list defines the IP address for the FortiGate.</p> <p>If you have not created a gateway list, this option is not available.</p>
---------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7. Click *Save*. The FortiClient installer is added to FortiClient EMS and displays on the *Manage Installers* pane.



If the *Sign software packages* option is enabled in *System Settings > Server*, Windows installers display as being from the publisher specified in the certificate file. See the *FortiClient EMS Admin Guide*.

Configuring endpoint profiles

When you install FortiClient EMS, a default profile is created. This profile is applied to any groups you create. The default profile is designed to provide effective levels of protection. To use specific features, such as application firewall, create a new profile or change the default profile.

Consider the following when creating profiles:

- Use default settings within a profile.
- Consider the endpoint's role when changing the default profile or creating new profiles.

- Create a separate group and profile for endpoints requiring long-term special configuration.
- Use FortiClient EMS for all central profile settings, and set options for within the group instead of for the endpoint itself when possible.

Creating profiles to deploy FortiClient

You must create a new profile to deploy FortiClient to endpoints. You cannot add a FortiClient installer to the default profile.

You must add FortiClient installers to FortiClient EMS before you can select the installers in a profile. See [Creating FortiClient installers on page 20](#).

The selected FortiClient installer in a profile controls what tabs are displayed for configuration in the profile. Only the tabs for the features in the selected installer are displayed for configuration in the profile. For example, if the installer includes only the VPN feature, only the *VPN* tab is displayed for you to configure. The *System Settings* tab always displays.

You can disable a feature included in the installer, then enable the feature in the profile later. For example, if the installer includes the Web Filter and VPN features, you can disable the Web Filter feature and keep the VPN feature enabled. When FortiClient is installed on the endpoint, the Web Filter is installed, but disabled.

1. Go to *Endpoint Profiles > Manage Profile*, and click the *Add* button.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient deployment options display.

3. Set the following options on the *Deployment* tab:

Action		
Assign an	Installer	Click <i>Installer</i> .
Installer		In the <i>Installer</i> list, select the desired FortiClient installer. The selected FortiClient installer affects what tabs display for configuration. Only tabs related to features enabled in the FortiClient installer display for configuration.
Schedule		
Start At		Specify what time to start installing FortiClient on endpoints.

	Reboot When Needed	Enable to reboot the endpoint to install FortiClient when needed.
	Reboot when no users is logged in	Enable to allow the endpoint to reboot without prompt if no endpoint user is logged into FortiClient.
	Notify users and let the user decide when to reboot when they are logged in	Enable to notify the end user if a reboot of the endpoint is needed and allow the user to decide what time to reboot the endpoint. Disable to reboot the endpoint without notifying the user.
Credentials		
	Username	Enter the username to perform deployment on AD. You must enter the admin credentials for the AD in the profile. Enter the appropriate credentials in the profile to assign to the AD. The credentials allow EMS to install FortiClient on endpoints using AD. If the credentials are wrong, the installation fails, and an error displays in EMS.
	Password	Enter the password to perform deployment on AD.

4. Set the options on the remaining tabs.
5. Click **Save**.

Importing FortiGate profiles

In FortiOS, endpoint profiles are called FortiClient Compliance profiles. You can import a FortiClient Compliance profile into EMS, then edit the profile in FortiClient EMS to add a FortiClient installer or add configuration information that supports the FortiGate compliance rules.



To import profiles successfully from FortiOS to FortiClient EMS, FortiGate must have the HTTPS port open. In FortiOS, go to *Network > Interfaces > Administrative Access* and enable the *HTTPS* checkbox.

1. Click *Endpoint Profiles > Manage Profiles > Import*. The *Import Profiles from FortiGate/FortiManager* window opens.

Import Profiles from FortiGate/FortiManager

Connect to FortiGate/FortiManager Preview and Select Configure Synchronization

Type

FortiGate FortiManager

Profile(s) will be imported as compliance rule(s)

IP address/Hostname

IP:Port

VDOM

root

Username

Required

Password

Quit Back Next Import

2. Under *Type*, select *FortiGate*.
3. Complete the following options, and click *Next*.

IP address/Hostname	Enter the IP address and port of the FortiGate device from which the profile is being imported, in the format: <ip address>:<port>.
VDOM	Enter a VDOM name from the FortiGate if applicable.
Username	Enter the FortiGate's login username.
Password	Enter the FortiGate's login password.

The list of FortiClient Compliance profiles configured on the FortiGate displays.

Import Profiles from FortiGate/FortiManager

Connect to FortiGate/FortiManager Preview and Select Configure Synchronization

☐ test

☒ Android </>

☒ Desktop </>

☐ iOS </>

☐ default

☐ Android </>

☐ Desktop </>

☐ iOS </>

Quit Back Next Import

Under each profile name is the list of profiles created for different operating systems, such as desktops running a Windows or macOS operating system or devices running an Android operating system. In the example, under the test profile, *Android*, *Desktop*, and *iOS* profiles are listed. You can click the </> icon beside each profile to preview the settings in XML format.

4. Select the profiles to import into EMS and click *Next*.

Select the name of the profile to import all profiles for it into EMS. You can also clear the checkbox beside the profiles you do not want to import into EMS. For example, you can import the Android and desktop profiles, but not the iOS profile for a given profile name.

5. Under *Synchronization Mode*, select one of the following options.

a. *One Time Pull*: If selected, FortiClient EMS does not automatically sync profile changes from the FortiGate. You can manually sync profile changes after importing the profile. See [0730_Sync profile changes on page 1](#).

b. *Group Schedule*: Select to configure a group synchronization schedule for all selected profiles. Select the next date and time to automatically update the profiles, and the profile update interval in days, hours, or seconds.

c. *Individual Schedule*: Select to configure an individual synchronization schedule for each selected profile. Select the next date and time to automatically update each profile, and the profile update interval in days, hours, or seconds.

6. Click *Import*. The selected profiles are imported into EMS and display under the *Endpoint Profiles* pane in a group named after the FortiGate device from which they were imported.

7. In the *Endpoint Profiles* page, select an imported profile to edit it.

The options configured in the profile by the FortiGate administrator are read-only compliance rules. You cannot change them. You can edit additional options to provide configuration information to support the compliance rules. You can also add a FortiClient installer to the profile by using the *Deployment* tab. Custom installers can be created. See [Creating FortiClient installers on page 20](#).

8. Edit the options on the tabs.

9. Click *Save Profile*.

Preparing Windows endpoints for FortiClient deployment

The following services must be enabled and configured on each Windows endpoint before FortiClient is deployed to them:

- Task Scheduler: Automatic
- Windows Installer: Manual
- Remote Registry: Automatic



The Windows Firewall must be configured to allow the following inbound connections:

- File and Printer Sharing (SMB-In)
- Remote Scheduled Tasks Management (RPC)

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually. You can locate the installer URL in *Manage Installers*. Go to *Profile Components > Manage Installers*.



When adding endpoints using an Active Directory domain server, FortiClient EMS automatically resolves endpoint IP addresses during initial deployment of FortiClient. FortiClient EMS can deploy FortiClient (Windows) to Active Directory endpoints that do not have FortiClient installed, as well as upgrade existing FortiClient installations if the endpoints are already connected to the EMS server.

Assigning profiles to Windows, macOS, and Linux endpoints

After creating the profile, you can assign the profile to domains or workgroups. When you assign the profile to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup.

If you do not assign a profile to a specific domain or workgroup, the default profile is automatically applied.

1. Go to *Endpoints*.
2. Right-click a domain or group, select *Assign profile*, then the profile. A confirmation dialog box displays.
3. Click *Yes*. The profile is assigned.

Viewing endpoints










After you add endpoints to FortiClient EMS, you can view the list of endpoints in a domain or workgroup in the *Endpoints* pane. You can also view details about each endpoint in the *Client Details* pane and use filters to access endpoints with specific qualities.

- [Viewing the Endpoints content pane on page 28](#)
- [Using the quick status bar on page 32](#)
- [Viewing endpoint details on page 33](#)
- [Filtering the list of endpoints on page 1](#)
- [Using bookmarks to filter the list of endpoints on page 1](#)

Viewing the Endpoints content pane

You can view information about endpoints on the *Endpoints* content pane.

1. Go to *Endpoints*, and select *All Endpoints*, a domain, or workgroup.
The list of endpoints in FortiClient EMS, a quick status bar, and a toolbar display in the content pane.


	0		0		0		0		1
Not Installed		Not Registered		Out-Of-Sync		Not Compliant		Security Risk	
<div> <div></div> <div>Search All Fields</div> <div>Filters</div> </div>									
Device	User	IP	Configurations	Connections	Status	Events			
 techdoc-fclient  Other Endpoints	qa	172.17.60.166	 Profile TEST	 Managed by EMS		<div> <div>AV 0</div> <div>SB 0</div> <div>FW 0</div> <div>VUL 46</div> <div>WEB 0</div> </div> <div>SYS 0</div>			

Not Installed	Number of endpoints that do not have FortiClient installed. Click to display the list of endpoints without FortiClient installed.
Not Registered	Number of endpoints not connected to FortiClient EMS or FortiGate. Click to display the list of disconnected endpoints.
Out-Of-Sync	Number of endpoints with an out-of-sync profile. Click to display the list of endpoints with out-of-sync profiles.
Not Compliant	Number of endpoints not compliant with the FortiGate compliance rules. Click to display the list of not compliant endpoints.
Security Risk	Number of endpoints that are a security risk. Click to display the list of endpoints.
Checkbox	Click to select all endpoints displayed in the content pane.
Show/Hide Heading	Click to hide or display the following column headings: <i>Device</i> , <i>User</i> , <i>IP</i> , <i>Configurations</i> , <i>Connections</i> , <i>Status</i> , and <i>Events</i> .
Show/Hide Full Group Path	Click to hide or display the full path for the group that the endpoint belongs to.
Refresh	Click to refresh the list of endpoints in the content pane.
Search All Fields	Enter a value and press <i>Enter</i> to search for the value in the list of endpoints.
Filters	Click to display and hide filters you can use to filter the list of endpoints.
Device	Visible when headings are displayed. Displays an icon to represent the operating system on the endpoint and the device name.
User	Visible when headings are displayed. Displays the name of the user logged into the endpoint.
IP	Visible when headings are displayed. Displays the endpoint's IP address.
Configurations	Visible when headings are displayed. Displays the name of the profile assigned to the endpoint and the profile's synchronization status.
Connections	Visible when headings are displayed. Displays whether the endpoint is connected to FortiClient EMS or FortiGate and the connection status of <i>Online</i> , <i>Offline</i> , or <i>Not Registered</i> .

Status	Visible when headings are displayed. Displays one of the following compliance statuses for the endpoint. <ul style="list-style-type: none"> • Compliant • Not compliant • Not participating in compliance • Quarantined • Excluded • Not registered • Not installed
Events	Visible when headings are displayed. Displays FortiClient events for the endpoint.

2. Click an endpoint to display its details in the content pane.

The following dropdown lists display in the toolbar for the selected endpoint:



Checkbox	Click to select and deselect all endpoints in the content pane. You can then select or clear the checkbox for individual endpoints to fine-tune the list of selected endpoints.
Scan	Click to start a Vulnerability or AntiVirus scan on the selected endpoint.
Patch	Click to patch all critical and high vulnerabilities on the selected endpoint. Choose one of the following options: <ul style="list-style-type: none"> • Selected Vulnerabilities on Selected Clients • Selected Vulnerabilities on All Affected Clients • All Critical and High Vulnerabilities
Action	Click to perform one of the following actions on the selected endpoint: <ul style="list-style-type: none"> • Upload FortiClient Logs • Request Diagnostic Results • Update Signatures • Re-register • De-register • Register • Quarantine • Un-quarantine • Exclude from Management • Mark as Uninstalled • Delete Device

The following tabs are available in the content pane toolbar when you select an endpoint, depending on which FortiClient features have been installed on the endpoint and enabled via the assigned profile:

Summary	Antivirus Events	Sandbox Events	Firewall Events	Vulnerability Events	Web Filter Events	System Events
---------	------------------	----------------	-----------------	----------------------	-------------------	---------------

Summary	
<user name>	Displays the name of the user logged into the selected endpoint. Also displays the user's avatar, email address, and phone number if these are provided to FortiClient on the endpoint. If the user's LinkedIn, Google, Salesforce, or other cloud app account is linked in FortiClient, the username from the cloud application displays.
Device	Displays the selected endpoint's device name.
OS	Displays the selected endpoint's operating system and version number.
IP	Displays the selected endpoint's IP address.
MAC	Displays the selected endpoint's MAC address.
Last Seen	Displays the last date and time that FortiClient sent a keep-alive message to EMS. This information is useful if FortiClient is offline because it indicates when the last keep-alive message occurred.
Location	Displays whether the selected endpoint is on-net or off-net.
Connection	Displays when the selected endpoint is connected to FortiClient EMS or FortiGate. Also displays the connection status.
Configuration	Displays the following information for the selected endpoint: <ul style="list-style-type: none"> • Profile: Name of the profile assigned to the selected endpoint • Installer: Name of the FortiClient installer used for the selected endpoint. Displays <i>Not Assigned</i> if no FortiClient installer has been assigned to the selected endpoint. • Gateway List: Name of the gateway list used for the selected endpoint. Displays <i>Not Assigned</i> if no gateway list has been assigned to the selected endpoint. • FortiClient Version: FortiClient version installed on the selected endpoint. • FortiClient Serial Number: Serial number for the selected endpoint's FortiClient license.
Compliance	Displays if the endpoint is compliant. If the endpoint is not compliant, displays the features for which FortiClient is not compliant.
Features	Displays which features are enabled for FortiClient.
Antivirus Events	
Date/Time	Displays the antivirus event's date and time.
Message	Displays the antivirus event's message.
Sandbox Events	
Date/Time	Displays the sandbox event's date and time.
Message	Displays the sandbox event's message.
Firewall Events	

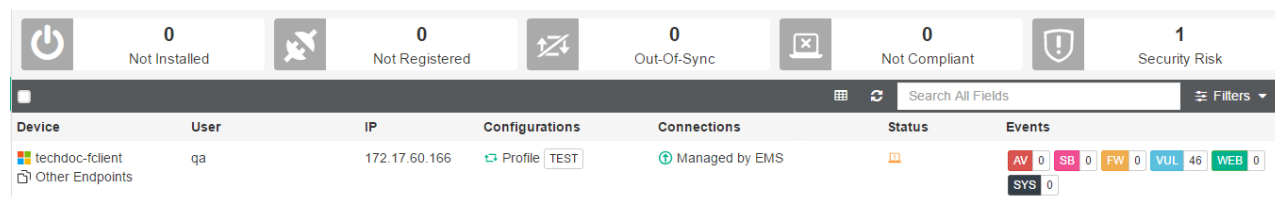
Date/Time	Displays the firewall event's date and time.
Message	Displays the firewall event's message.
Vulnerability Events	
Vulnerability	Displays the vulnerability's name. For example, <i>Security update available for Adobe Reader</i> .
Category	Displays the vulnerability's category. For example, <i>Third Party App</i> .
Application	Displays the name of the application with the vulnerability.
Severity	Displays the vulnerability's severity.
FortiGuard ID	Displays the FortiGuard ID number. If you click the FortiGuard ID number, it redirects you to FortiGuard where further information is provided if available.
Bulletin	Displays a link to a bulletin about the software vulnerability.
Web Filter Events	
Date/Time	Displays the web filter event's date and time.
Message	Displays the web filter event's message.
System Events	
Date/Time	Displays the system event's date and time.
Message	Displays the system event's message.

Using the quick status bar

You can use the quick status bar to quickly display filtered lists of endpoints on the *Endpoints* content pane.

1. Go to *Endpoints*.
2. Click *All Endpoints*, a domain, or workgroup.

The list of endpoints and quick status bar display.



3. Click one of the following buttons in the quick status bar:
 - Not Installed
 - Not Registered
 - Out-Of-Sync
 - Not Compliant
 - Security Risk

The list of affected endpoints displays.
4. Click an endpoint to display its details.

5. In the *Events* column, click the *AV <number>*, *SB <number>*, *FW <number>*, *VUL<number>*, *WEB <number>* and *SYS<number>* buttons to display the associated tab of details for the selected endpoint.
6. Click the *Total* button to clear the filters.
The unfiltered list of endpoints displays.

Viewing endpoint details

You can view each endpoint's details on the *Endpoints* content pane. For a description of the options on the *Endpoints* content pane, see [Viewing the Endpoints content pane on page 28](#).

1. Go to *Endpoints*, and select *All Domains*, a domain, or workgroup.
The list of endpoints for the selected domain or workgroup displays.
2. Click an endpoint to display details about it in the content pane.
Details about the endpoint display in the content pane.

The screenshot displays the FortiClient EMS interface. At the top, there are status indicators for various components: Not Installed (0), Not Registered (0), Out-Of-Sync (0), Not Compliant (0), and Security Risk (1). Below these are tabs for Scan, Patch, and Action. A search bar and a Filters button are also present.

Device	User	IP	Configurations	Connections	Status	Events
WIN-1F3BOCJBRAM	Administrator	10.0.4.102	Profile: Default	Managed by EMS		VUL 14

Below the table, there are tabs for Summary, Vulnerability Events, and System Events. The **Summary** tab is selected, showing details for the user **Administrator**.

Device WIN-1F3BOCJBRAM

OS Microsoft Windows Server 2012 ...

IP 10.0.4.102

MAC 0a-bb-d5-7b-14-c8

Last Seen 9/13/2018, 6:07:24 PM

Location On-Net

Connection

Managed by EMS

Configuration

Profile	Default
Installer	Not Assigned
Gateway List	Not Assigned
FortiClient Version	6.0.2.0128
FortiClient Serial Number	FCT8003586546796

Compliance

Features

- AntiVirus installed
- Sandbox Detection installed
- Web Filter installed
- Application Firewall installed
- Remote Access configured
- Vulnerability Scan enabled
- SSOMA installed

FortiClient EMS for Chromebooks Setup

This section describes how to set up FortiClient EMS for Chromebooks. Following is a summary of how to set up FortiClient EMS for Chromebooks:

1. Add an SSL certificate. See [Adding SSL certificates on page 47](#).
2. Add the Google domain. See [Adding Google domains on page 48](#).
3. Create an endpoint profile. See [Adding new profiles on page 48](#).
4. Assign the endpoint profile to the Google domain. See [Assigning profiles to Chromebooks on page 50](#).
5. View the status. See [Viewing domains on page 50](#).

Additional configuration procedures are also included in this section.

Google Admin Console setup

This section describes how to add and configure the FortiClient Web Filter extension on Chromebooks enrolled in the Google domain.

Following is a summary of how to set up the Google Admin console:

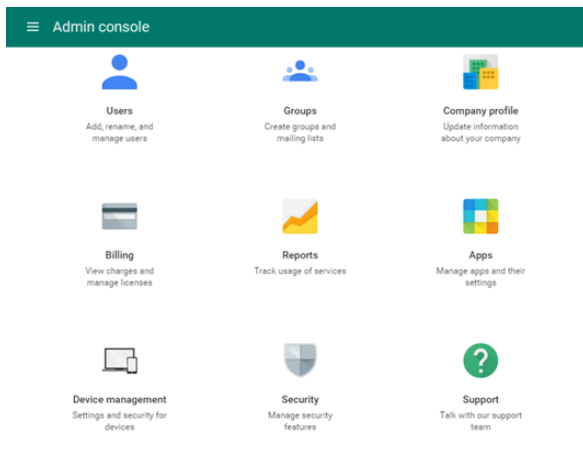
1. Log into the Google Admin console. See [Logging into the Google Admin console on page 34](#).
2. Add the FortiClient Web Filter extension. See [Adding the FortiClient Web Filter extension on page 35](#).
3. Configure the FortiClient Web Filter extension. See [Configuring the FortiClient Web Filter extension on page 35](#).
4. Add the root certificate. See [Adding root certificates on page 36](#).



If you are using another Chromebook extension that uses external rendering servers, the FortiClient Web Filter settings may be bypassed. Check with the third-party extension vendor if this is the case.

Logging into the Google Admin console

Log into the [Google Admin console](#) using your Google domain admin account. The Admin console displays.



Adding the FortiClient Web Filter extension

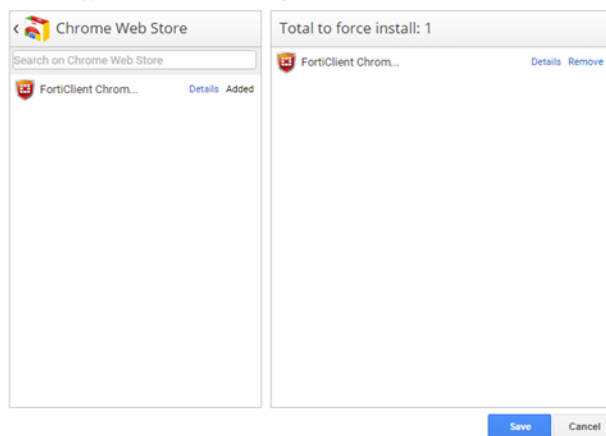


FortiClient EMS software is not available for public use. You can only enable the feature using the following extension ID: `igbgpehnbmhdgjbhkkpedommgmfbear`

1. In the Google Admin console, go to *Device management > Chrome Management > User Settings > Apps and Extensions > Force-installed Apps and Extensions > Manage force-installed apps*.
2. Select *Chrome Web Store*, and search for the following extension ID: `igbgpehnbmhdgjbhkkpedommgmfbear`.
3. Add the extension ID and save.

The extension name displays as *FortiClient Chromebook Web Filter Extension*.

The selected apps and extensions will be automatically installed.



Configuring the FortiClient Web Filter extension

You must configure the FortiClient Chromebook Web Filter extension to enable the Google Admin console to communicate with FortiClient EMS.

FortiClient EMS hosts the services that assign endpoint profiles of web filtering policies to groups in the Google domain. FortiClient EMS also handles the logs and web access statistics sent from the FortiClient Web Filter extensions.



FortiClient EMS is the profile server.

1. In FortiClient EMS, locate the server name and port by going to *System Settings > Server*.
2. Create a text file that contains the following text:

```
{  
  "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >" }  
}
```

For example:

```
{  
  "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443" }  
}
```
3. In the Google Admin console, go to *Device management > Chrome Management > App Management > FortiClient Chrome Web Filter Extension > User settings*.
4. Click a domain or organization unit (OU).
5. In the right pane, under *Configure*, upload a new configuration file.
You can also view the current settings.
6. Click *Save*.
7. Go to *Device Management > Chrome > App Management* to view your configured Chrome apps.

Adding root certificates

This section includes the following information.

- [Communication with the FortiClient Chromebook Web Filter extension on page 36](#)
- [Communication with FortiAnalyzer for logging on page 37](#)
- [Summary of where to add certificates on page 37](#)
- [Uploading root certificates to the Google Admin console on page 38](#)

Communication with the FortiClient Chromebook Web Filter extension

The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add it to FortiClient EMS to allow the extension to trust FortiClient EMS.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS. See [Adding SSL certificates to FortiClient EMS for Chromebook endpoints on page 47](#).

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiClient EMS and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS will not work. See [Uploading root certificates to the Google Admin console on page 38](#).

Communication with FortiAnalyzer for logging

This section applies only if you are sending logs from FortiClient EMS to FortiAnalyzer. If you are not sending logs, skip this section.



Sending logs to FortiAnalyzer requires you enable ADOMs in FortiAnalyzer and add FortiClient EMS to FortiAnalyzer. FortiClient EMS is added as a device to the FortiClient ADOM in FortiAnalyzer. See the *FortiAnalyzer Administration Guide*.

FortiClient EMS supports logging to FortiAnalyzer. If you have a FortiAnalyzer device and configure FortiClient EMS to send logs to FortiAnalyzer, a FortiAnalyzer CLI command must be enabled and an SSL certificate is required to support communication between the FortiClient Web Filter extension and FortiAnalyzer.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer. See [Adding SSL certificates to FortiAnalyzer](#).

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiAnalyzer and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer will not work. See [Uploading root certificates to the Google Admin console on page 38](#).



The FortiAnalyzer IP address should be specified in the SSL certificate. If you are using a public SSL certificate, the FortiAnalyzer IP address can be assigned to *Common Name* or *Alternative Name*. If you are using a self-signed (nonpublic) SSL certificate, your certificate's *Subject Alternative Name* must include `IP:<FortiAnalyzer IP>`.

You must use the FortiAnalyzer CLI to add HTTPS-logging to the allow-access list in FortiAnalyzer. This command is one step in the process that allows FortiAnalyzer to receive logs from FortiClient EMS.

In FortiAnalyzer CLI, enter the following command:

```
config system interface
  edit "port1"
    set allowaccess https ssh https-logging
  next
end
```

Summary of where to add certificates

The following table summarizes where to add certificates to support communication with the FortiClient Web Filter extension and FortiAnalyzer.

Scenario	Certificate and CA	Where to add certificates
Allow the FortiClient Chromebook Web Filter extension to trust EMS	Public SSL certificate	<ul style="list-style-type: none"> Add SSL certificate to FortiClient EMS.
	SSL certificate not from a common CA	<ul style="list-style-type: none"> Add SSL certificate to FortiClient EMS. Add your certificate's root CA to the Google Admin console.

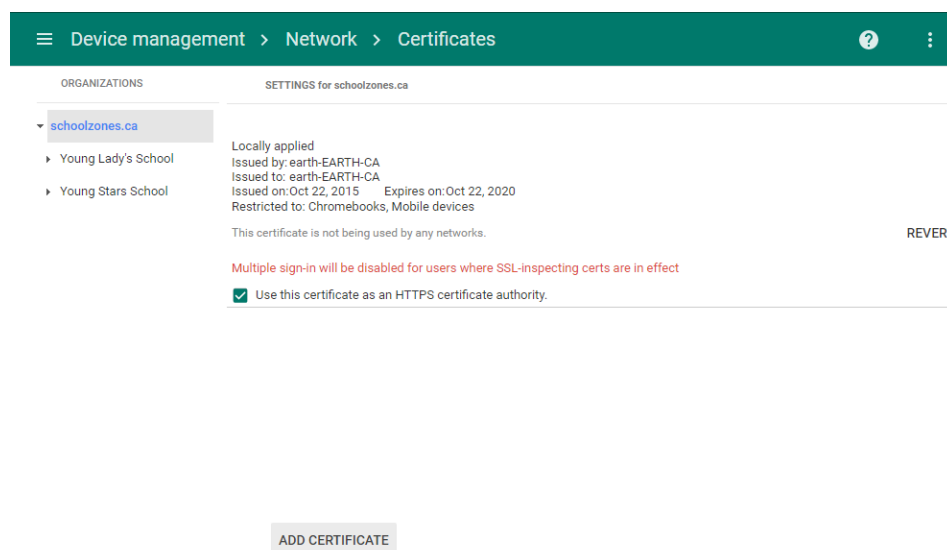
Scenario	Certificate and CA	Where to add certificates
Allow the FortiClient Chromebook Web Filter extension to trust FortiAnalyzer for logging	Public SSL certificate	<ul style="list-style-type: none"> Add SSL certificate to FortiAnalyzer.
	SSL certificate not from a common CA	<ul style="list-style-type: none"> Add SSL certificate to FortiAnalyzer. Add your certificate's root CA to the Google Admin console.

Uploading root certificates to the Google Admin console

1. In the Google Admin console, go to *Device Management > Network > Certificates (root certificate) (cert certificate)*.
2. Add the root certificate.
3. Select the *Use this certificate as an HTTPS certificate authority* checkbox.



Do not forget to select the *Use this certificate as an HTTPS certificate authority* checkbox.



Disabling access to Chrome developer tools

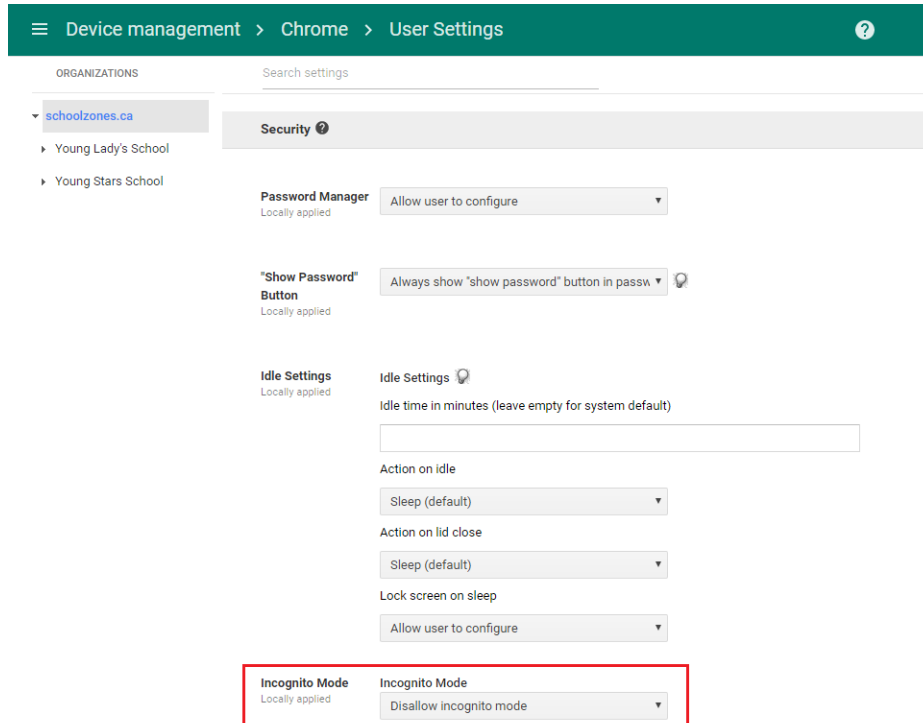
It is recommended to disable access to Chrome developer tools. This blocks users from disabling the FortiClient Web Filter extension.

1. In the Google Admin console, go to *Device management > Chrome Management > User Settings*.
2. For the *Developer Tools* option, select *Never allow use of built-in developer tools*.

Disallowing incognito mode

When users browse in incognito mode, extensions are bypassed. Incognito mode should be disallowed for managed Google domains.

1. In the Google Admin console, go to *Device management > Chrome management > User settings*.
2. From the left panel, select the organization.
3. In the *Security* section, set *Incognito Mode* to *Disallow incognito mode*.



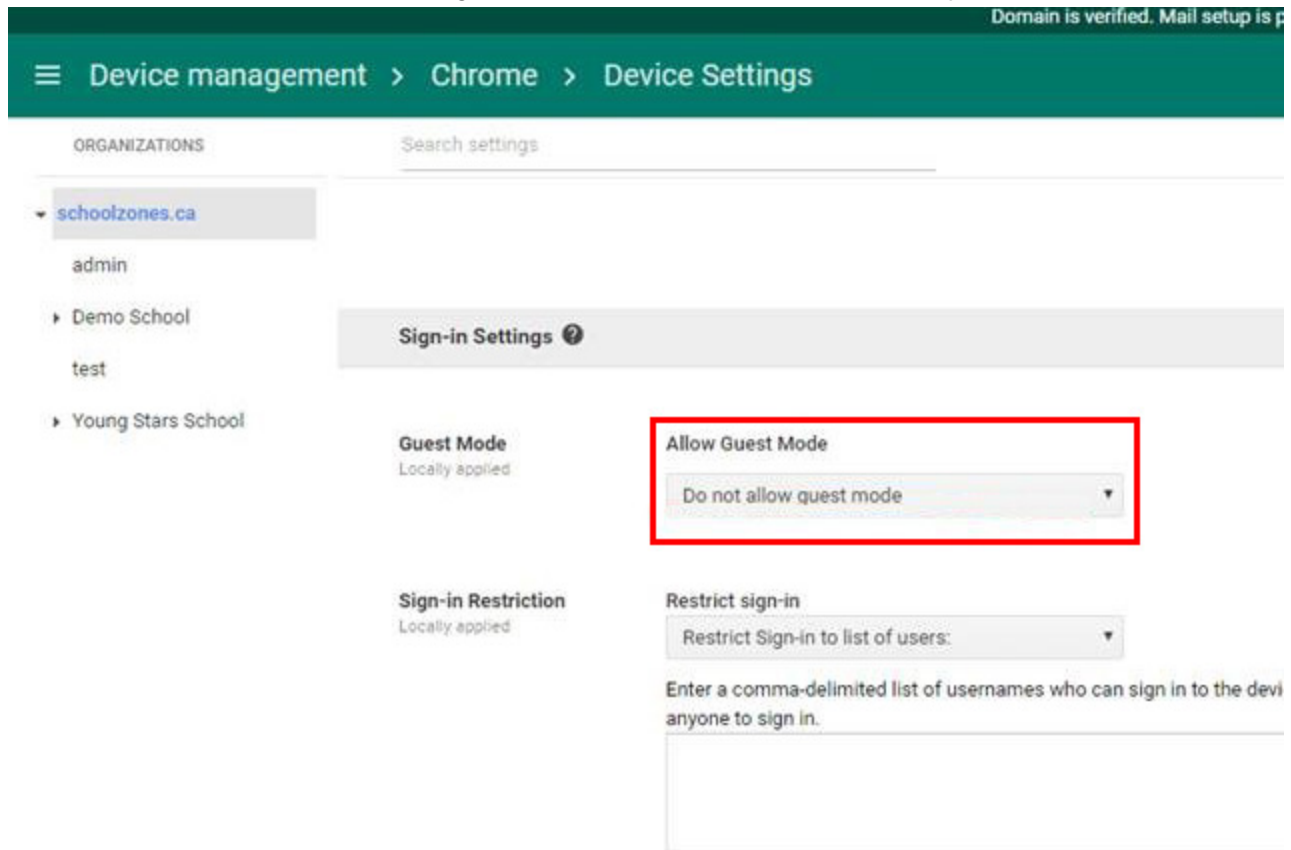
4. Click **Save**.

Disallowing guest mode

Guest mode should be disallowed for managed Google domains.

1. In the Google Admin console, go to *Device management > Chrome management > Device settings > Sign-in settings*.
2. From the left panel, select the organization.

- Under *Guest Mode*, select *Do not allow guest mode* from the *Allow Guest Mode* dropdown list.

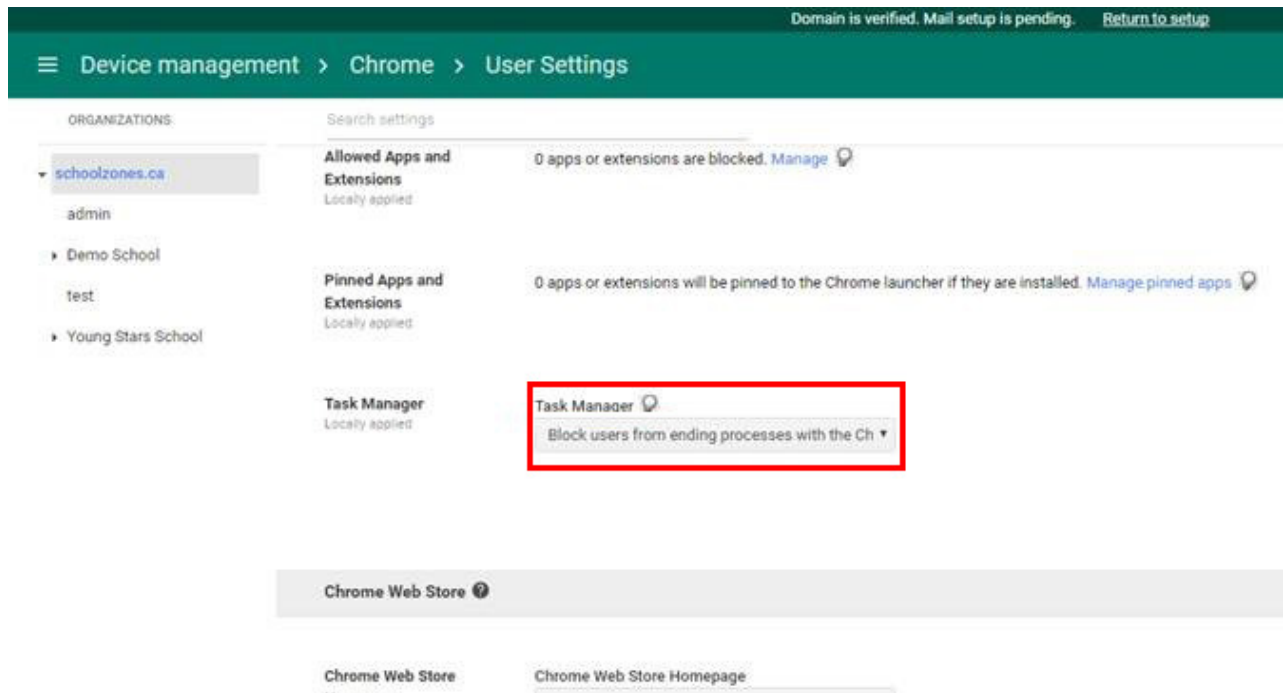


- Click **Save**.

Blocking Task Manager

Task Manager should be blocked for managed Google domains.

- In the Google Admin console, go to *Device Management > Chrome Management > User settings > Apps and Extensions*.
- From the left panel, select the organization.
- Under *Task Manager* select *Block users from ending processes with the Chrome Task Manager* from the dropdown list.



4. Click Save.

Service account credentials

FortiClient EMS requires service account credentials generated by the Google Developer console. You can use the default service account credentials provided with FortiClient EMS or generate and use unique service account credentials, which is more secure.



The service account credentials must be the same in FortiClient EMS and the Google Admin console.

This section describes how to configure default and unique service account credentials. See the following sections.

Configuring default service account credentials

FortiClient EMS includes the following default service account credentials generated by the Google Developer console:

Option	Default setting	Where used
Client ID	102515977741391213738	Google Admin console
Email address	account-1@forticlientwebfilter.iam.gserviceaccount.com	FortiClient EMS

Option	Default setting	Where used
Service account certificate	A certificate in .pem format for the service account credentials	FortiClient EMS



The service account credentials are a set. If you change one credential, you must change the other two credentials.

Adding the default service account client ID to the Google Admin console

To configure the default service account credentials, you must add the client ID's default value to the Google Admin console. No other configuration for service account credentials is required. See [Adding service account credentials to the Google Admin console on page 46](#).

Configuring unique service account credentials

When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS:

1. Create unique service account credentials using the Google Developer console. See [Creating unique service account credentials on page 42](#).
2. Add the unique service account credentials to the Google Admin console. See [Adding service account credentials to the Google Admin console on page 46](#).
3. Add the unique service account credentials to FortiClient EMS. See [Adding service account credentials to EMS on page 46](#).

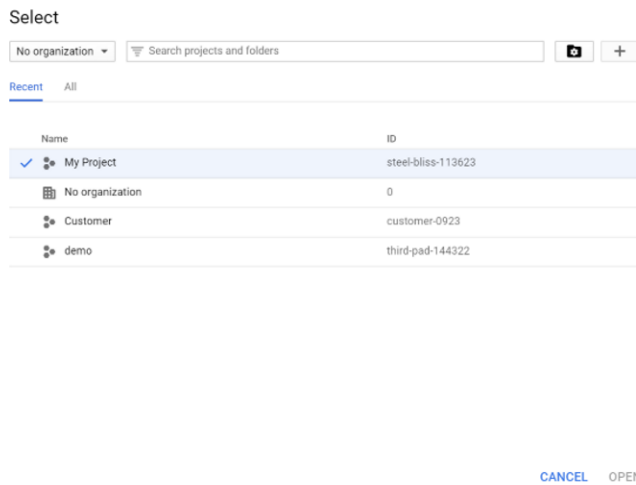
Creating unique service account credentials

Creating a unique set of service account credentials provides more security. Unique service account credentials include the following:

- Client ID (a long number)
 - Service account ID (email address)
 - Service account certificate (a certificate in .pem format)
1. Go to [Google Cloud Platform](#).
 2. Log in with your G Suite account credentials.

3. Create a new project:

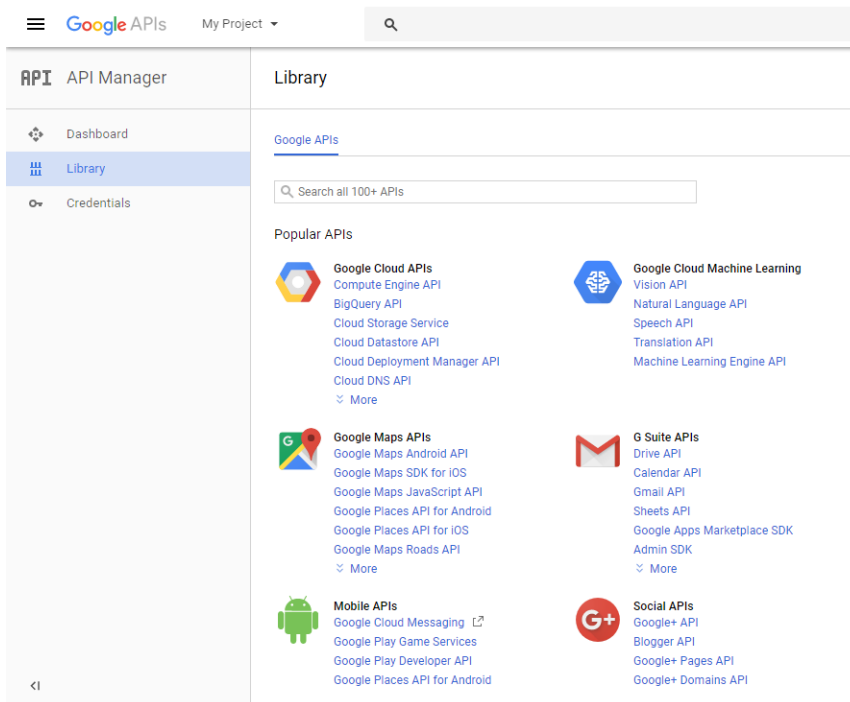
- a. Click the toolbar list. The browser displays the following dialog.



- b. Select your organization, if you see an organization dropdown list.
- c. Click the + button.
- d. In the *Project name* field, enter your project name, then click *Create*.

4. Enable the Admin SDK:

- a. Select your project from the toolbar list, then go to the *Library* tab.
- b. Under *G Suite APIs*, click *Admin SDK*.



c. Click **ENABLE**.

The screenshot shows the Google APIs Admin SDK page. The left sidebar has a menu with 'API Manager', 'Dashboard', 'Library', and 'Credentials'. The main content area is titled 'Admin SDK' and has a red box around the 'ENABLE' button. Below the title, there is a section 'About this API' with a description: 'Admin SDK lets administrators of enterprise domains to view and manage resources like user, groups etc. It also provides audit and usage reports of domain.' There are two diagrams: 'Using credentials with this API' showing a flow from 'Your app' to 'User consent' to 'User data', and 'Server-to-server interaction' showing a flow from 'Your service' to 'Authorization' to 'Google service'.

5. Create a service account:

- Go to the *Credentials* tab and select *Create Credentials > Service account key*.
- From the *Service account* list, select *New Service Account*. Enter a service account name.
- From the *Role* list, select *Project > Viewer*.
- Select *P12* as the *Key type* and click *Create*.

The screenshot shows the 'Create service account key' form. The left sidebar has a menu with 'API Manager', 'Dashboard', 'Library', and 'Credentials'. The main content area is titled 'Create service account key'. There is a 'Service account' dropdown menu with 'New service account' selected. Below it, there is a 'Service account name' input field with 'test' and a 'Role' dropdown menu with 'Viewer' selected. Below that, there is a 'Service account ID' input field with 'test-410' and '@voltaic-facet-170220.iam.gserviceaccount.com'. Below the 'Service account ID' field, there is a 'Key type' section with two radio buttons: 'JSON' (Recommended) and 'P12' (For backward compatibility with code using the P12 format). The 'P12' radio button is selected. At the bottom, there are 'Create' and 'Cancel' buttons.

After you create the service account, a private key with the P12 extension is saved on your computer.



The private key with the P12 extension is the only copy you will receive. Keep it in a safe place. You should also remember the password prompted on the screen. At this time, that password should be **notasecret**.



To use the private key in EMS, it needs to be converted to `.pem` format. You can use the following `openssl` command to convert it. Remember to use the `notasecret` password.

```
C:\OpenSSL-Win64\bin>openssl pkcs12 -in demo-976b9d6e9328.p12 -out
serviceAccount-demo.pem -nodes -nocerts
Enter Import Password:
```

Adding service account credentials to the Google Admin console

This section describes how to add the client ID from the service account credentials to the Google Admin console. These settings allow Google to trust FortiClient EMS, which enables FortiClient EMS to retrieve information from the Google domain.

1. In the Google Admin console, go to *Security > Advanced settings > (you may need to click "show more" to see this) > Manage API client access*.
2. Set the following options:
 - a. For the *Client Name* option, add the client ID from the service account credentials.
 - b. For the *API Scopes* option, add the following string:
`https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly`



The API scopes are case-sensitive and must be lowercase. You may need to copy the string into a text editor and remove spaces created by words wrapping to the second line in the PDF.

3. Click *Authorize*.

Adding service account credentials to EMS

The section describes how to add the service account ID and service account certificate from the service account credentials to FortiClient EMS.

1. In FortiClient EMS, go to *System Settings > EMS for Chromebook*.



The default service account credentials display. Overwrite the default settings with the unique set of service account credentials received from Fortinet.

2. The *Service account* field shows the configured email address provided for the service account credentials. Click the *Update service account* button and configure the following information:

ID	Enter a new email address for the service account credentials.
Private key	Click <i>Browse</i> and select the certificate provided with the service account credentials.

3. Click *Save*.
4. Update the client ID in the Google Admin console.



The service account credentials are a set. If you change one credential, you must change the other two credentials.

Adding SSL certificates

This section includes information about the required SSL certificates to support the following types of communication:

- [Communication with the FortiClient Chromebook Web Filter extension on page 36](#)
- [Communication with FortiAnalyzer for logging on page 37](#)

It includes the following procedures:

- Required: [Adding SSL certificates to FortiClient EMS for Chromebook endpoints on page 47](#)
- Required only when sending logs to FortiAnalyzer: [Adding SSL certificates to FortiAnalyzer on page 48](#)

Adding SSL certificates to FortiClient EMS for Chromebook endpoints

You must add an SSL certificate to FortiClient EMS to allow Chromebooks to connect to EMS.

If you are using a public SSL certificate, add the certificate to FortiClient EMS. You do not need to add the certificate to the Google Admin console.

If you are not using a public SSL certificate, you must add the SSL certificate to FortiClient EMS, and the root certificate to the Google Admin console. See [Adding root certificates on page 36](#).

1. In FortiClient EMS, go to *System Settings > Server > EMS for Chromebooks Settings*.
2. Do one of the following:
 - a. To replace an existing SSL certificate, beside *SSL certificate*, click *Update SSL certificate*.
 - b. If no SSL certificate has been added yet, click the *Upload new SSL certificate* button.
3. Click *Browse* and locate the certificate file (<name>.pfx).
4. In the *Password* box, enter the password.
5. Click *Test*.
6. Click *Save*.



If the SSL certificate is expiring in less than three months, the expiry date label is yellow; if it has expired, the label is red. Otherwise, it is green.

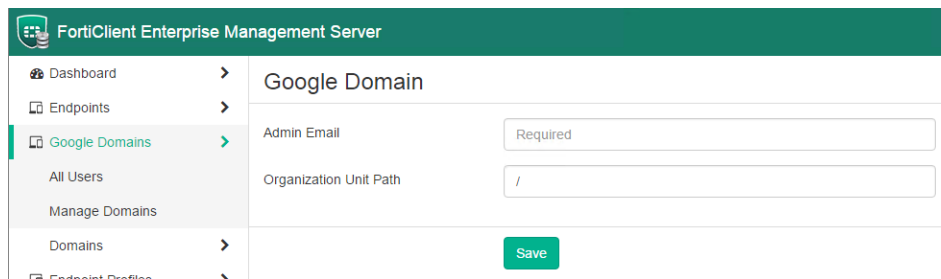
SSL Certificate	server2.pfx 5/12/2019
New SSL Certificate File	<input type="text" value="Browse..."/>
New SSL Password	<input type="text" value="Required"/>

Adding SSL certificates to FortiAnalyzer

1. In FortiAnalyzer, go to *System Settings > Certificates > Local Certificates*.
2. Click *Import*. The *Import Local Certificate* dialog appears.
3. In the *Type* list, select *Certificate* or *PKCS #12 Certificate*.
4. Beside *Certificate File*, click *Browse* to select the certificate.
5. Enter the password and certificate name.
6. Click *OK*.

Adding Google domains

1. Go to *Google Domains > Manage Domains*, and click the *Add* button. The *Google Domain* pane displays.



The screenshot shows the FortiClient Enterprise Management Server interface. On the left is a navigation menu with options: Dashboard, Endpoints, Google Domains (highlighted), All Users, Manage Domains, Domains, and Endpoint Profiles. The main area is titled 'Google Domain' and contains two input fields: 'Admin Email' with a 'Required' label and 'Organization Unit Path' with a '/' label. A green 'Save' button is at the bottom right of the form.

2. In the *Admin Email* box, enter your Google domain admin email.
3. In the *Organization Unit Path* box, enter the domain organization unit path.



/ stands for the root of the domain.

4. Click *Save*.
The Google domain information and users are imported into FortiClient EMS.

Configuring Chromebook profiles

Chromebook profiles support web filtering by categories, black and white lists, and safe search. You can create different profiles and assign them to different groups in the Google domain.

Adding new profiles

When you install FortiClient EMS, a default profile is created. This profile is applied to any domains you add to FortiClient EMS.



It is recommended to add Yandex search engine to the black list in the profile.

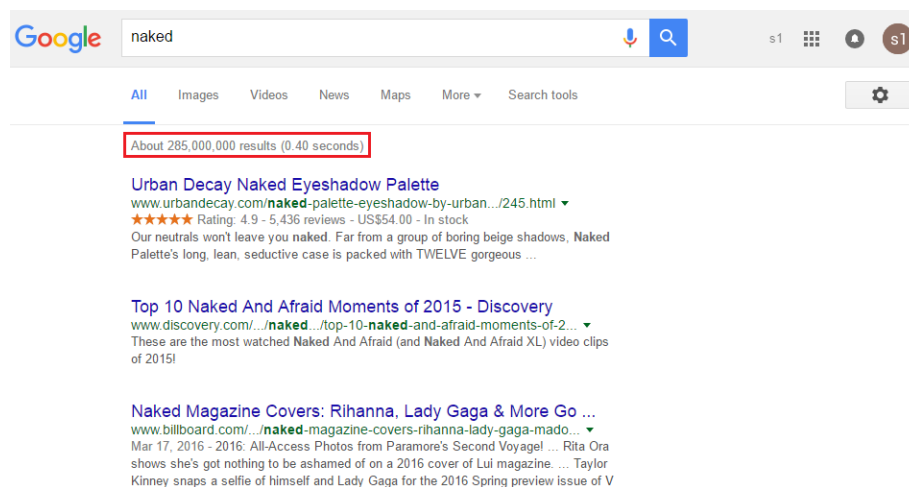
1. Go to *Endpoint Profiles > Manage Profiles*, and click the *Add Chrome* button.
2. In the *Profile Name* box, enter the profile name.
3. On the *Web Filter* tab, enable *Web Filter*, and set the web filtering options.
4. On the *System Settings* tab, set the logging options.
5. Click *Save*.

Enabling/disabling safe search

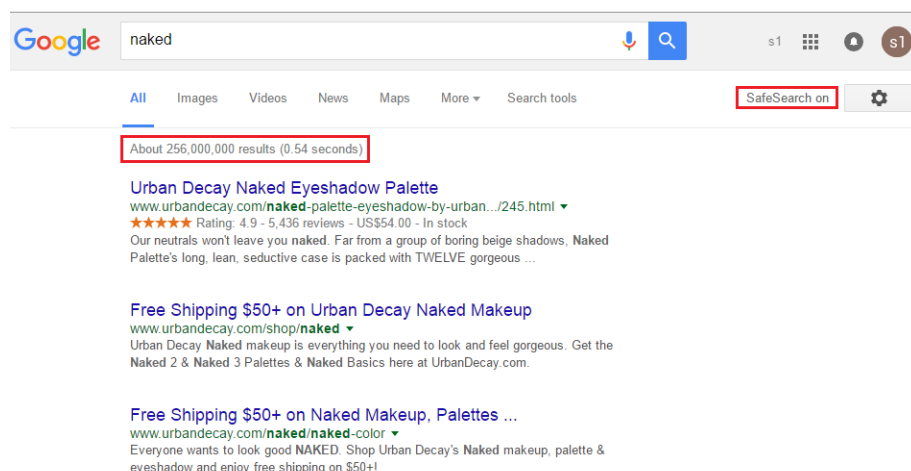
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS controls the Safe Search feature.

Following are examples of search results with the Safe Search feature disabled and enabled. Notice the difference between the number of results. Here are the search results when the Safe Search feature is disabled, which has about 285000000 results:



Here are the search results when the Safe Search feature is enabled, which has about 256000000 results.



1. In FortiClient EMS, in the *Endpoint Profiles > Manage Profiles* area, click the *Default - Chromebooks* profile or another profile.
2. On the *Web Filter* tab, enable or disable *Enable Safe Search*.

Assigning profiles to Chromebooks

After creating the profile, you can assign the profile to Google domains. When you assign the profile to domains, the profile settings are automatically pushed to the Chromebooks in the domain.

1. Go to *Google Domains*.
2. Right-click a domain, select *Assign Profile*, then the profile. The profile is assigned.
3. Hover the mouse over the name of the domain to view the name of the assigned profile.

Viewing domains

After you add domains to FortiClient EMS, you can view the list of domains in *Google Domains*. You can also view the list of Google users in each domain and details about each Google user in the *User Details*, *Client Statistics*, and *Blocked Sites* panes.

Viewing the Google Users pane

You can view Google users' information in FortiClient EMS.

1. Go to *Google Domains > Domains* and click a domain. The list of Google users displays.

Google Users Clear Filters Refresh					
Name	Email	Last Login	Last Policy Retr	Domain	Organization Path
Art3 Sikes	art3.sikes@s...	8/4/2016 1:1...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
bob bob	bob.bob@ys...	8/6/2016 1:0...	Never Retrie...	schoolz...	/test
Catherine Seely	Catherine.Se...	7/25/2016 9:...	Never Retrie...	schoolz...	/Young Stars School
Dean Cagle	Dean.Cagle...	8/5/2016 10:...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
Dennis Auger	Dennis.Auger...	7/15/2016 9:...	Never Retrie...	schoolz...	/Young Lady's School/students...
Edgar Bayles	Edgar.Bayles...	8/9/2016 12:...	Never Retrie...	schoolz...	/Young Stars School/students/...
Efrain2 Tague	Efrain2.Tagu...	8/2/2016 10:...	Never Retrie...	schoolz...	/Young Stars School/students/...
Emilio Freitag	emilio.freitag...	7/25/2016 9:...	Never Retrie...	schoolz...	/Young Lady's School/students...
Garry Heinrich	Garry.Heinric...	8/3/2016 8:2...	Never Retrie...	schoolz...	/Young Lady's School/staff/admin
Gerard Rhoa...	gerard.rhoad...	7/14/2016 11...	Never Retrie...	schoolz...	/Young Lady's School/staff
jiaping xu	jpxu@school...	8/9/2016 6:4...	Never Retrie...	schoolz...	/
Joey Albrecht	joey.albrecht...	8/2/2016 10:...	Never Retrie...	schoolz...	/Young Lady's School/staff
KeriNew Coc...	Keri.Cochran...	8/4/2016 1:1...	Never Retrie...	schoolz...	/Young Lady's School/test
Leann Bast	Leann.Bast@...	8/9/2016 12:...	Never Retrie...	schoolz...	/Young Stars School/students/...

The following options are available in the toolbar:

Clear Filter (filter icon)	Click the Clear Current Filter icon to clear the currently used filter.
Refresh	Click the Refresh icon to refresh the page.

The following columns of information are displayed for Google users:

Name	Chromebook user's name.
Email	Chromebook user's email address.
Last Login	Date and time when the user last logged into the domain.
Last Policy Retrieval	Date and time of the last endpoint profile retrieved by the Google Chromebook.
Domain	Name of the domain to which the user belongs.
Organizational Path	Organization path in the domain.

Viewing user details

You can view details about each user in a Google domain.

1. Go to *Google Domains > Domains*. The list of domains displays.
2. Click a domain. The list of Google users displays.
3. Click a Google user and scroll to the bottom of the content pane. The *User Details*, *Client Statistics*, and *Blocked Sites* panes display.

User Details

Field	Information
Name	User's name.
Email	User's email address.
Last Login	Date and time when the user last logged into the domain.
Last Policy Retrieval	Date and time of the last endpoint profile retrieved by the Google Chromebook.
Organization Path	Organization path of the user in the domain.
Effective Policy	Name of the profile assigned to the user in the domain.

Client Statistics

Charts	Information
Blocked Sites Distribution (past <number> days)	Displays the distribution of blocked sites in the past number of days. You can configure the number of days for which to display information. Go to <i>System Settings > Logs</i> .
Top 10 Site Categories by Distribution (Past <number> Days)	Displays the distribution of top ten site categories in the past number of days. You can configure the number of days for which to display information. Go to <i>System Settings > Logs</i> .

Blocked Sites (Past <number> Days)

Fields	Information
Time	Time the blocked site was visited.
Threat	Threat type detected.
Client Version	Chromebook user's current version.
OS	Type of OS used by the Chromebook user.
URL	Blocked site's URL.
Port	Port number currently listening.
User Initiated	User initiated visitation to the blocked site.

Change Log

Date	Change Description
2018-10-18	Initial release.
2018-11-06	Updated Required services and ports on page 6 .
2018-11-23	Added note to Google Admin Console setup on page 34 .



FORTINET®



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.